Head Office: PSSSF Millennium Towers II, Bagamoyo Road
P.O Box. 9300, Dar es Salaam, Tanzania
Telephone: +255 22 2162940 Fax: +255 22 2114815
website: www.tcbbank.co.tz
Emal: ceo@tcbbank.co.tz

Tanzania Commercial Bank is a Bank that provides competitive financial services to our customers and creates value for our stakeholders through innovative products.

Tanzania Commercial Bank is a Bank, whose vision is "to be the leading bank in Tanzania in the provision of affordable, accessible and convenient financial services". As part of effective organizational development and management of its human capital in an effective way, Tanzania Commercial Bank commits itself towards attaining, retaining and developing the highly capable and qualified workforce for Tanzania Commercial Bank betterment and the Nation at large.

ICT OFFICER (CYBERSECURITY)-1 POSITION

Tanzania Commercial Bank seeks to appoint dedicated, self-motivated and highly organized **ICT Officer (Cybersecurity) 1 position** to join the Directorate of Technology

DIRECT REPORTING LINE	Senior Manager ICT Security and BCP
LOCATION	Head Office
WORK SCHEDULE	As per Tanzania Commercial Bank Staff regulations
SECTION	ICT Security
SALARY	Commensurate to the Job Advertised

POSITION OBJECTIVES

- To assist Senior Manager ICT Security and BCP and Director of Technology to drive information technology security strategy.
- To protect the organization's data and systems using sophisticated tools, instrumentation, and knowledge of Information Technology (IT) to monitor, evaluate, and manage Cyber risks.
- To identify current threats, mitigate vulnerabilities, and anticipate future cybersecurity challenges.
- To utilize the new technology which will increase the security of our existing and emerging IT systems.

KEY RESPONSIBILITIES

- Perform audit and security compliance checks, including network penetration testing, vulnerability scans, and other configuration analysis.
- Lead the ICT team and consult them on the remediation of security vulnerabilities.

- Hunt cybersecurity threats and mitigate them before they compromise the organization.
- Implement appropriate security tools and systems to uncover potential threats before they turn into attacks.
- Develop cyber threat models and security risk assessments and recommend mitigations and countermeasures to address risks, vulnerabilities, and threats.
- Conduct Malware monitoring, analysis, and reverse engineering.
- Perform Information Security Incident Handling and Digital Forensic Investigations.
- Analyze network traffic for intrusions and cyberattacks in both parameter and internal networks.
- Monitoring and analyzing events and alerts from a wide array of security devices and systems (SIEMs, Firewalls, IDS/IPS, WIPS, Systems, Networks, Anti-virus, etc.)
- Administer Security Incident and Event Management system(SIEM) and ensure all mission-critical systems are well-integrated.
- Take Part in the software development lifecycle and uncover potential flaws before and after deployment.
- Formulate and review IT Security controls following best practice benchmarks for applications, operating systems, network devices, storage, databases, and endpoints.
- Implement Cyber controls as stipulated in the policies and procedures.
- Assisting in the development of security compliance reports such as ISO27001, PCI DSS, and more as directed from time to time.
- Perform cybercrime incident coordination, analysis, and response in

collaboration with the authorities and the internal fraud unit.

- Access and document the damage caused by security breaches and report to all stakeholders.
- Prepare security alerts and warnings to the users and interested parties.
- Maintains technical knowledge by attending educational workshops; reviewing publications.
- As part of the team, support security initiatives through predictive and reactive analysis and articulating emerging trends to management and staff.
- Perform any other related information security duties assigned from time to time.

Education and Experience

- Bachelor's degree/Advanced Diploma in Information Technology, Computer science, Cybersecurity, Information Technology, Computer Engineering or any other related discipline from recognized University.

- Should have a minimum of two years' experience of ICT technology with at least hands-on technical roles in cybersecurity security, digital forensics, or information security.

Competency and skills:

- Ability to work in a fast-paced environment.
- Problem-solving and decision-making skills.
- Good communication and sound interpersonal skills.
- Exceptional verbal and written skills.
- Ability to prioritize tasks and to work independently or in a group as needed.
- Fundamental knowledge and understanding of TCP/IP, routing, firewall, switching, and hands-on experience using tcpdump or Wireshark.
- Network Mapping and cyber analytics.
- Knowledge of or experience with SIEM, DAM, IPD/IDS monitoring technologies
- Working knowledge of the Linux, Unix, and Windows operating systems.
- Experience working on a cyber-security incident response team.
- Working knowledge of various web servers and web technologies and application-layer.
- Knowledge of scripting languages and Python programming language is a bonus.

- Knowledge of Relational Database Management Systems such as Oracle, MSSQL, MySQL, and SQL language.
- Working knowledge of public key infrastructure and encryption systems.
- High levels of integrity in the conduct of personal and professional affairs.
- Professional Certification such as CISSP, CEH, CPENT, CCNA Security is an added advantage.
- The capability of conducting threat hunting, vulnerability assessment, and penetration testing.

The position will attract a competitive salary package, which include benefits. Applicants are invited to submit their resume via the following link:-

https://www.tcbbank.co.tz/careers **Applications via other methods will not be considered. Applicants need to fill their personal information, academic certificates and work experiences and also submit the application letter. Other credentials will have to be submitted during the interview for authentic check and other administrative measures.**

Tanzania Commercial Bank has a strong commitment to environmental, health and safety management. Late applications will not be considered. Short listed candidates may be subjected to any of the following: a security clearance; a competency assessment and physical capability assessment.

AVOID SCAMS: NEVER pay to have your application pushed forward.
Any job vacancy requesting payment for any reason is a SCAM. If you are requested to make a payment for any reason, please use the Whistle blower policy of the Bank, or call 0222162940 to report the scam. You also don't need to know one in Tanzania Commercial Bank to be employed. Tanzania Commercial Bank is merit based institution and to achieve this vision, it always go for the best.

Deadline of the Application is 31st July, 2023.